UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH 949-280-2025, 901-206-8795, 317-446-6758, 901-871-7236 THAT IS STORED AT PREMISES CONROLLED BY AT&T

Case No. 4:13-MJ-294

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Northern District of Texas, Fort Worth Division, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1958	Use of interstate commerce facilities in commission of murder-for-hire

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Michael C. Elsey
Applicant's signature

Michael Elsey, FBI, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/29/13

J. Cureton
Judge's signature

City and state: Fort Worth, Texas

United States Magistrate Judge Jeffrey L. Cureton
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Michael C. Elsey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by AT&T, a wireless provider headquartered at 1 AT&T Plaza, 208 S. Akard Street, 10th Floor, Dallas, Texas 75202. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require AT&T to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since May, 1986. I have participated in numerous investigations in which cellular telephones have been utilized to communicate with other subjects and/or victims in order to perpetrate a crime or track victims. These communications have been made through voice calls, text messages, and E-mails. Victims may have received text messages or voice mails from subjects who have directly threatened the victim or have communicated with the victim in order to determine the location of the victim. Cellular telephones may store this type of evidence that can be vital to the identification of individuals who commit various crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1958, the use of interstate commerce facilities in the commission of murder-for-hire have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

5. On May 22, 2013, at approximately 6:47 PM, Juan Jesus Guerrero Chapa, hereinafter referred to as the victim, was shot as he returned to his vehicle parked at the Southlake Town Square, 100 Grand Avenue, Southlake, Texas, by an unknown assailant. The victim and his wife, Julia Maria Tijerina De La Garza, arrived at Southlake Town Square at approximately 6:00 PM and parked in a parking space across from the Yumilicious Yogurt Shop. The victim and his wife went into Yumilicious and then sat on a bench in Southlake Town Square in front of their vehicle. The victim and his wife then walked around Southlake Town Square and were observed to enter Nine West store and purchase shoes. The victim and his wife walked back to their vehicle. The victim's wife went to the driver's side of the vehicle and the victim went to the passenger side of the vehicle. As the victim was getting into the passenger side of the vehicle, a white Sports Utility Vehicle (SUV) was observed to slowly drive to the back of victim's vehicle and a lone male, wearing a hooded sweatshirt with the hood pulled up

and a scarf or bandanna over his nose and mouth, exited the back passenger side door of the SUV. The unknown male had a gun with a possible suppressor attached to it. The unknown male shot at the victim in the passenger seat of his vehicle at least nine times. The unknown male re-entered the white SUV through the back passenger door and the white SUV left the area. The victim was deceased at the scene. The victim had two cellular telephones, 901-206-8795 and 317-446-6758 on his person and one cellular telephone, 949-280-2025, in the vehicle, at the time of the murder. The victim's wife identified the above cellular telephones as belonging to the victim. A fourth cellular telephone, 901-871-7236. was identified as being used by the victim, after law enforcement conducted a consent to search of the victim's residence. Any text messages and voice mail messages are being sought for the cellular telephones that were owned and utilized by the victim, in order to determine if the victim received any direct threats or unusual messages from the unknown subjects.

6. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for AT&T subscribers may be located on the computers of AT&T. Further, I am aware that computers located at AT&T contain information and other stored electronic communications belonging to unrelated third parties.

7. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of AT&T for weeks or months.

8. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging" or "wireless messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by AT&T for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

9. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

10. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

11. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

12. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the

dates and times of payments and the means and source of payment (including any credit card or bank account number).

13. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

14. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require AT&T to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

15. Based on the forgoing, I request that the Court issue the proposed search warrant.

16. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, 18 U.S.C. § 2711(3)(A)(i).

17. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Michael C. Elsey
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 29th day of May, 2013 at 3:00 a.m./p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with 949-280-2025, 901-206-8795, 317-446-6758, 901-871-7236 that is stored at premises owned, maintained, controlled, or operated by AT&T, a wireless provider headquartered at 1 AT&T Plaza, 208 S. Akard Street, 10th Floor, Dallas, Texas 75202.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by AT&T

To the extent that the information described in Attachment A is within the possession, custody, or control of AT&T, including any messages, records, files, logs, or information that have been deleted but are still available to AT&T or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), AT&T is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;

b. All existing printouts from original storage of all of the text messages described above;

c. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;

d. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S.C. § 1958, the use of interstate commerce facilities in the commission of murder-for-hire involving unknown individuals during an indeterminate period of time, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by AT&T, and my official title is _____. I am a custodian of records for AT&T. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of AT&T, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of AT&T; and

c. such records were made by AT&T as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature